The cause/consequence diagram method as a basis for quantitative accident analysis

Nielsen, Dan S.

Publication date:
1971

Document Version
Publisher's PDF, also known as Version of record

Risö-M-1374

Risö-M-1374

Danish Atomic Energy Commission

Research Establishment Risö

ELECTRONICS DEPARTMENT

The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis

by

Dan S. Nielsen

May 1971

R-5-71

A. E. K. Risø

Risø - M - [illegible]

Risø - M - 1374

Title and author(s)

The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis

by

Dan S. Nielsen

Date May 1971

Department or group

Electronics Department

Group's own registration number(s)

R-5-71

17 pages + tables + 10 illustrations

Abstract

A graphical method for clearing up relevant accidents in complex nuclear installations is presented. The method is a proposal for an expedient presentation of the logical connections between a "spectrum" of accident causes and a "spectrum" of relevant consequences, e.g. expressed in terms of fission products released to the population. Besides being a tool used in connection with the clearing-up of these consequences and their causes, the method serves as a basis from which the probability of occurrence of the individual consequences may be evaluated.

The main principle of the method involves the concept of a "critical event", which for example may often be described as a transgression of the safety limit of a vital reactor parameter, followed by two fault tree methods used in a combined way to determine the logical connections between the causes of the critical event and the "incredible", but possible, consequences of it.

Copies to

Abstract to

Available on request from the Library of the Danish Atomic Energy Commission (Atomenergikommissionens Bibliotek), Risø, Roskilde, Denmark. Telephone: (03) 35 51 01, ext. 334, telex: 5072.

Fi 25-204

ISBN 87 550 0084 3

CONTENTS

Page

Summary..... 2

Introduction..... 4

1. Formulation of Requirements to the Graphical Tool used in Connection with Quantitative Accident Analysis..... 4

2. Methods for Clearing-Up and Presentation of Accidents..... 6
   2.1. The Cause Diagram Method..... 6
   2.2. The Consequence Diagram Method..... 9

3. Discussion..... 12

4. Probability Analysis in Connection with use of the Cause/Consequence Diagram Method..... 15

5. References - Literature..... 17

Summary: The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis

The purpose of this paper is the presentation of a graphical method for clearing up relevant accidents in complex nuclear installations. Generally expressed the method is a proposal for an expedient presentation of the logical connections between a "spectrum" of accident causes and a "spectrum" of relevant consequences, e.g. expressed in terms of fission products released to the population. Besides being a tool used in connection with clearing up these consequences the method serves as a basis from which the probability of occurrence of the individual consequences may be evaluated.

Presented are the logical connections between essential foreseeable failure causes, failure courses and their consequences in cases where they are terminated as intended, and not terminated as intended. As an accident is the result of a coincidence of events and/or failures, fault trees with the logical "AND" and "OR" gates are used in such a way that the following relevant items are stated:

1. Relevant failure causes (including causes of common mode failures and human failures).
2. Logical connections between events and conditions.
3. Time delays in the single failure courses where these delays are significant.
4. Relevant consequences.

Together with the concept a "critical event", which for example may often be described as a transgression of the safety limit of a vital reactor parameter, the main principle of the method is that two fault tree methods are used in a combined way to determine the logical connections between the causes of the critical event and the possible consequences of it.

The "cause diagram" (cause searching) is the well-known fault tree where the construction of the tree begins with the definition of the "top" undesired event (the critical event). The causes are then indicated and connected with the top event by means of a logic gate, and the procedure is repeated for each of the causes until all events have been fully developed.

The "consequence diagram" (consequence searching) is an event-sequential diagram showing the alternative courses the critical event might lead to if one or more systems with accident-anticipating/limiting effect do not function as intended. Cause diagrams, normally evaluated for the worst functional failure of these systems, are coupled to the consequence diagram.

INTRODUCTION

For the solution of the problems in connection with the use of a more quantitative approach at the safety assessment of nuclear power plants it is necessary that expedient tools for accident analysis should be available and employed during the design phase as well as at the final safety assessment of the plant. Tools that in a systematic way can handle large systems and be helpful at the display of the factors that are of vital importance for the safety.

The purpose of this paper is the presentation of a proposal for a graphical accident analysis method which is based on the use of a combination of already existing graphical tools for accident analysis.

1. FORMULATION OF REQUIREMENTS TO THE GRAPHICAL TOOL USED IN CONNECTION WITH QUANTITATIVE ACCIDENT ANALYSIS

For a more quantitative approach to be carried out at the safety assessment of a nuclear power station it is necessary to have a methodology that can be used in connection with analysis of accidents in large complex systems. A methodology which can partly elucidate the ability of the plant to meet and subdue accident situations and which can partly determine a representative spectrum of accidents that, if they occur, will have serious radiological consequences for the personnel and the population. This spectrum of accidents can subsequently be taken as a starting point for assessment of the "safety degree" of the plant, and the question whether this is adequate or not has to be answered. The quantitative approach together with some safety criteria lead to an objective answer to this question (ref. 1).

One of the necessary conditions for a realistic quantitative analysis is, however, that it is possible to give a sufficiently broad description and presentation of the logical connections between a "spectrum" of accident causes and a "spectrum" of relevant accident consequences, the latter for instance expressed in terms of quantitative specifications of fission products released to the surroundings.

A given accident can be said to be characterized by a "cause", a sequence of events where the time between the occurrence of the single events can be an important parameter, and finally by the consequences of the accident. A graphical method for clearing up relevant accidents should therefore be worked out as a tool that can be used at the determination of the alternative possible courses and consequences that the (postulated) "cause" might lead to if one or more of the accident-anticipating/limiting provisions fail. Furthermore, the method should provide a basis for determination of the probabilities of the single consequences.

As to the regarded failure or event, called the "cause" of the accident, some problems concerning the cause specification might arise. Is it for instance expedient in some cases to define the "cause" as a transgression of the "safety limit" of a vital reactor parameter and in other cases as a critical functional failure in an important system. In the latter case, on which "level" should it then be chosen, on a "sub-system level",..... or a "component level"? In short, the question is: What is the most expedient starting point of an accident analysis?

It is, of course, not possible a priori directly to define neither the possible relevant consequences nor the causes which might lead to these. Starting an analysis by an arbitrary choice of a cause such as an accidental closure of a valve, or a certain temperature regulator failure, and then trying to find out what can happen, seems to be both overwhelmingly difficult and unexpedient.

In a graph connecting all relevant causes and consequences it may be found that the paths from several independent causes to their consequences have a "common node" in the form of a certain event beyond which the graphs are indentical. This means that it may be more expedient as a starting point to postulate a certain event, related to the node, that may be a result of many independent causes, and that calls for actions from the same accident-anticipating/limiting systems. This event may be considered as a "critical event" from which a consequence-searching as well as a cause-searching analysis may be performed.

Summing up, this means that by means of the graphical tool the logical connections between essential foreseeable failure causes, failure courses and their consequences in cases that are terminated as intended, and not terminated as intended, should be presented in such a way that the following relevant items are stated:

1. Relevant failure causes (including causes of common mode failures and human failures).
2. Logical connections between events and conditions.
3. Time delays in the single failure courses where these delays are significant.
4. Relevant consequences.

2. METHODS FOR CLEARING-UP AND PRESENTATION OF ACCIDENTS

As an accident is the result of a coincidence of events and/or failures, fault trees with the logic AND and OR gates are used. The diagram methods hitherto used can on the whole be divided into two main groups that may be called:

1. The cause diagram method (cause searching).
2. The consequence diagram method (consequence searching).

2.1. The Cause Diagram Method

The cause diagram is an event logic diagram relating events and conditions to a particular undesired event which might be for instance a relevant system failure, see fig. 1. Only events that might contribute to the undesired event are considered.

The method is characterized by the following points:

1. The construction of the diagram begins with a precise definition of the "top" undesired event, i.e. the system failure of interest.
2. The tree is then developed downwards, i.e. the causes of the "top" event are connected with this by means of a logic gate, and the procedure is repeated for each of the causes and the causes of the causes until all events have been fully developed. The tree is considered fully developed when all independent causes, the basic input events, have been identified.

3. In principle the cause diagram or certain especially important parts of it can be developed down to independent failures of such components as bolts, relays, transistors, etc., but normally one stops at a higher level where the components comprise pumps, valves, measuring channels, etc. Occasionally also subsystems or equipment failures are used as basic input events if they are independent of all other basic input events.

4. At each gate used in the diagram the input events must always be both necessary and sufficient, in the context of the gate, to produce the output event, otherwise the diagram will not be valid for probability analysis.

5. Through the use of logic gates the cause diagram is very suitable for revealing single failures as well as combinations of failures which might lead to the undesired event, and the purpose is to bring to light not only "hardware" failures, but also "software" causes such as human failures.

Generally, at the development of a cause diagram, special attention should be directed towards identification of common mode failures, i.e. simultaneous failures of two or more functionally independent system parts from a common cause.

When redundant functional units are used, the probability that all, or nearly all, fail because of random internal faults may be made extremely small if all failures of the units are independent. In practice a system with so-called redundant units may, however, contain a not recognized and accepted common element, and a failure of this might cause failure of the entire system, i.e. a common mode failure (the design and analysis may be incomplete, and an unknown or undetected causal relation exists between failures that are hypothesized as independent or even incredible). Common mode failures of this kind may especially in systems with accident-anticipating/limiting intervention function often remain unrevealed until a thorough test of the system function is carried out. A cause diagram analysis may be hoped to reveal at least some of the causes of such failures and by this bring about a redesign. If the failure possibility is accepted, however, the analysis may help at an assessment or improvement of the test and maintenance procedures.

The worst category of common mode failures may arise, however, under accident conditions where the performance of systems with accident-

anticipating/limiting intervention function is of great importance. A functional failure of a normal operation system may initiate the need for reactor protection. If the same circumstances can also induce failure of the instrumentation that was provided to protect against the failure, a potentially hazardous situation exists. Similar, or particularly identical, functional units are susceptible to such common mode failures, and it is not evident that the probability of all of the units failing as the result of a single external or "environmental" event is acceptably small.

The environmental factors (external causative conditions) that have in practice been the cause of common mode failures may be divided into the following categories (see ref. 2 in which examples are presented):

1. Change in characteristics of the system being protected (e.g. long term temperature changes).

2. Unrecognized dependence on a common element.

3. Disability caused by the accident being guarded against.

4. Human error.

The symbols used in connection with development of a cause diagram should in a systematic way help the analyst to direct the attention towards an identification of all the possible causes that may lead to a regarded functional system/equipment/component failure. Particularly to direct the attention towards identification of common mode failures an expedient failure classification, that may be applied to any regarded "unit level", would in this respect be valuable.

Symbols presented in ref. 3 have been adopted, see fig. 2. Of logic gates only the AND and the OR gates are used. To classify the failure modes of a functional unit these are categorized as either "primary", "secondary", or "input". The OR gate (fig. 2) means that failure in just one of these categories is sufficient to make the output event occur.
Primary failure occurs under normal operation conditions and may be brought about by inadequate design, a defect or deterioration in service. The symbol is a circle (a termination symbol).
Secondary failure occurs when the object is subjected to unintended influence from other structurally and operationally separated systems/equipment/components in which failures have occurred (damage caused for instance by a crane, by missiles from exploded components, by temperature, pressure, vibration, humidity, or radiation influences during accident conditions). The symbol is a diamond (a termination symbol).

Input failure occurs when the functional unit is directed to fail, either by the imposition of excessive process conditions (out of control), mechanical loads, false signals (including also noise signals), false directions from operator/personnel (e.g. wrong set point - or trip level - setting, etc.), or loss of power supply in those cases where this is also a supply to other functional units. The symbol is a rectangle, which indicates events or conditions which might be further developed.

A common mode failure may be either a secondary failure or an input failure.

In fig. 3 a cause diagram is developed for a simple pump stand-by system with manual switch-over to the stand-by unit P2 if loss of the normal "P1-flow" occurs. Loss of the P1-flow should be recognized by the operator by reading either the pressure transducer D1 or the dif. pressure transducer D2. It is assumed that both motor pumps are supplied from a common guaranteed supply, whereas the motor-driven valves V1 and V2 are supplied from independent sources.

The undesired event is defined as "total loss of pump flow", and the diagram provides a basis for determination of the probability that the undesired event will occur at least once during a certain operating time, T.

Generally special attention should be directed towards identification of common mode failures. In the simple example mentioned loss of the guaranteed supply can be regarded as the cause of a common mode failure which, as shown in fig. 3, should be explicitly shown (loss of the electric supply for V1 for instance can be regarded as belonging to a primary failure category).

2.2. The Consequence Diagram Method

The other graphical method, the consequence diagram method, is a tool which can be used at the clearing-up of the logical connections between a postulated critical event and the possible relevant consequences of this event, see fig. 1. By use of expedient symbols the method can furthermore be helpful at the determination of the probability of the single consequences. The principle of the method is that the starting point is the definition of a critical event, and the objective is to describe how the accident might arise in spite of all precautions to prevent it.

The diagram in fig. 4 shows the important items that it is necessary to subject to an analysis by use of the consequence diagram method. Normally, for each regarded critical event a number of different possibilities of release of fission products to personnel and population are present. To define all relevant consequences of this kind it is, however, necessary to make a quite general clearing-up of consequences, where all possible operator faults and faulty conditions in systems and/or equipment with accident-anticipating/limiting function are included in the analysis and combined with cases where operator and/or systems/equipment function correctly. A systematic clearing-up of these relationships will thus identify all possible results, inclusive of the cases where fission product release from the fuel does not result in radiological consequences, and the cases where fission product release does not occur at all.

If the facts are included that a manual intervention may be more or less effective (the time that passes before the intervention is realized is for instance a factor which may have decisive influence), or that a system/equipment has failed, but is all the same more or less capable of carrying out the function intended, then a clearing-up might give a number of "continuous spectra" of relevant consequences (one may thus imagine that one or more areas within all degrees of fuel damage and fission product release to the surroundings may occur).

In practice, however, one has to base the logical diagrams on limitations that are often stringent with the result that a "discrete spectrum" of consequences is a more apt designation. The consequence diagram method is then characterized by the use of the following methodology:

1. The starting point is an examination of all relevant operating conditions with reference to a definition of critical events, i.e. events which may separately lead to fission product release from the fuel (the condition for release to the surroundings), if one or more of the accident-anticipating/limiting provisions fail. A critical event may often be defined within a certain category of functional failures in the systems or equipment which are primarily necessary for establishment of the desired operation conditions. The limiting values of fuel temperature, coolant outlet temperature, power in relation to flow, etc., often dictate the working ranges of the system functions. The limits of such "dictated" working ranges may therefore often constitute the fault criteria.

In some cases it may also be expedient to define the critical event as a transgression of the "safety limit" of a vital reactor parameter due to system function failures.

2. For each critical event a logical clearing-up of connections between events and conditions is carried out in order to determine the possible alternative accident consequences. For each system or equipment with accident-anticipating/limiting function, only two states are normally taken into account. These states are 1) correct system functioning and 2) worst functional system failure (example: control rod trip - no control rod trip).
   In the same way a distinction is made between 1) correct manual intervention (i.e. intervention which carried out in accordance with established procedures gives an intended accident-anticipating or -limiting effect) and 2) no manual intervention.

3. As was the case with the cause diagram method, different graphical symbols are used. Symbols which, if they are expedient, force the analyst at least qualitatively to follow up and present the possible sequences. When the complete qualitative diagram is present, the analyst is to quantify the consequences and their probability. The quantitative determination of the consequences, i.e. the fission products released to the surroundings, may for instance be based on mathematical model calculations of the possible energy transients. In so doing, the character and the extent of fuel damage, which make up the starting point for the further assessment, are determined.

Graphical symbols that are very suitable for use in connection with the consequence diagram method have been proposed by Mr. O. Knecht and Mr. H. Keil, see ref. 6. Among the proposed symbols, see fig. 5,(some of the symbols are in this paper slightly modified),especially the "delay" symbol should be noticed. By means of this the time parameter, which may often be an important factor at the determination of the consequences, is introduced. In the probability analysis the time that passes between important sequential events (the delay) is important as the knowledge of critical delays may often help the analyst to differentiate the different courses in the right way.

In fig. 6 a consequence diagram for the critical event "drop of control rod" (BWR) is partly developed.

3. DISCUSSION

The necessary basis for use of a more quantitative approach in connection with the safety assessment of a nuclear power plant is a definition and presentation of the logical connections between a "spectrum of independent accident causes" and a "spectrum of relevant accident consequences".

On the question how the causes, which at worst could lead to fission product release from the fuel, are identified, one might be tempted to think that the cause diagram method (cause searching) alone would be the right method. That this is not correct can be seen when it is taken into consideration that the cause diagram method is based on a precise definition of an undesired event. Fuel damage constitutes an undesired event, but it would be impossible a priori to define the character and the extent of the damage which might occur.

It seems, however, reasonable, when the problem is to define and connect the two spectra, to use a combination of the cause diagram and the consequence diagram methods. Among the symbols shown in fig. 5, the rectangular symbol with the mutually exclusive outputs "no" and "yes" is often in connection with the function of a system or an item of equipment used to indicate the two states "functions correctly" and "does not function". As the "no" output represents a well-defined failure condition, it provides an expedient coupling point between the consequence diagram and the cause diagram of the system/equipment failure concerned.

Often the causes of a critical event may be determined by means of the cause diagram method. In principle the input-output data of the total "combined diagram" of a certain critical event will by this method be as shown in fig. 7.

The cause diagrams whose outputs are inputs to the consequence diagram may conveniently be divided into:

1. Cause diagrams of functional failures in systems or equipment that are primarily necessary to establish the desired operation conditions (BWR: reactor vessel, control systems, main steam and feed water lines, main condenser, turbine/generator + grid, etc.).

2. Cause diagrams of the normally "worst" functional failures in systems/equipment with accident-anticipating/limiting function (automatic trip systems, emergency power supplies, emergency heat removal systems,

clean-up systems, containment, etc.; if desired, certain control systems for normal operation may in some cases be included in this category).

The structure of a cause/consequence diagram is shown in fig. 8. From the different kinds of symbols reference can be made to supporting information concerning operating and emergency instructions, test and maintenance procedures, component analysis, fault effect analysis, etc.

As mentioned earlier a critical event is an event which may lead to fission product release from the fuel if one or more systems/equipment with accident-anticipating/limiting function fail. Each normal operating condition of the reactor should therefore be analysed for critical events which may lead to the following main categories of accidents:

1. Reactivity accidents
2. Loss of coolant
3. Loss of coolant flow.

For a given reactor condition and main category of accident the steps in an analysis may generally be as follows:

1. Postulation of a critical event that may be a result of several independent causes, and that calls for actions from the same systems with accident-anticipating/limiting intervention function. The critical event may for instance be defined as a transgression of the safety limit of a vital reactor parameter due to several (hypothesizedly) independent system/sub-system/component failures.

2. Definition of other critical events on the basis of the cause/consequence diagram for the postulated critical event.

   a) The cause/consequence diagram of the postulated critical event focuses the single system/sub-system/component function failure. This may be regarded as a critical event that occurs when the function under consideration transgresses the limits of a prescribed working range dictated by consideration of the fuel protection.
   Normally a critical event may be defined as a functional failure in a normal operation system/sub-system/component, but in some cases also functional failures of certain accident-anticipating/limiting systems may be relevant (example: accidental closure of main steam isolation valves in a BWR).

   b) The symbols used for secondary and input failure modes of a functional unit should bring about a thorough examination of the possibility of unrecognized causal relations between the "hypothesizedly independent" system/sub-system/component failures that might cause the postulated critical event. In so doing, other critical events may be found (example: loss of a certain energy supply may cause simultaneous failure of several of the systems under consideration. The loss of this energy supply is a critical event, which furthermore perhaps also significantly influences other systems/sub-systems/components than those hitherto regarded).

   c) The secondary and input failure mode symbols should help particularly to direct the attention towards identification of events (causes) that during accident conditions can induce catastrophic failure of a system with accident-anticipating/limiting intervention function. The combination of an operation system failure and a "blockade" failure of the mentioned kind should be treated separately as a critical event.

3. For each of the critical events a cause/consequence diagram is developed. It may sometimes be necessary, however, to treat different sub-cases of the critical event in order to obtain consequence diagrams with well-defined time delays. (The performance of the single accident-anticipating/limiting intervention system has to be assessed, and the important question to be answered is: Does the system fulfil the basic objectives under the conditions to be met?) The criterion is that only those independent faults that may yield identical or nearly identical consequences (transient studies may show this) are taken into account at the development of the cause/consequence diagram. If all such independent causes of the sub-case of the critical event are determined, the "sub-case" itself can be regarded as an independent event connected with a probability distribution function.

In this paper the term "a system or equipment with accident-anticipating/limiting function" has been used instead of the term "an engineered safety system". Normally "an engineered safety system" is defined as a safety feature not required for normal operation. In this way a distinction is made between safety properties due to design, operation and maintenance, and features added to cope specially with accidents. In accordance with sound engineering practices an operational and structural separation

between normal operation systems and "safety systems" is therefore aimed at. However, for a given plant the question of what systems are regarded as safety systems arises, and a specification of these might perhaps to a great extent restrict the possibilities for selection of critical events. In order to meet the demands for safety and production reliability (availability) some of the normal operation control systems might in certain cases be used for less radical accident-anticipating intervention (intervention which for instance gives a certain smaller power reduction an by this brings the reactor in a safe state). The term "a system with accident-anticipating/limiting function" may include such control systems, and the possibility of inclusion of these in a consequence diagram is thus kept open.

4. PROBABILITY ANALYSIS IN CONNECTION WITH USE OF THE CAUSE/CONSEQUENCE DIAGRAM METHOD

The cause/consequence diagram method can be used as a basis for probability analysis of large complex systems as well as of small systems. For illustration of how a probability analysis may be carried out the earlier treated stand-by pump system is chosen as an example.

The concept a "critical event" is for the sake of illustration used, and it is defined as "stop of P1-flow". As accident consequence is regarded "total stop of pump flow". In fig. 9 the cause/consequence diagram is shown with calculations for determination of the probability P(T) that total stop of pump flow will occur at least once during a certain operating time, T. As seen, the probability distribution function $P_d(t)$ constitutes the basis from which P(T) is determined. The function $P_d(t)$ may be regarded as a distribution function of "demands" where demands generally expressed are considered to be those undesired events which call for some immediate or almost immediate action to carry out a required protective function. As the cause of the common mode failure, loss of the common electric supply for the pumps, has been "extracted" from the cause/consequence diagram and shown separately, $P_d(t)$ is given by:

$$P_d(t) = P_{P1}(t) \cdot (1 - P_e(t)),$$

where $P_{P1}(t)$ is the distribution function of the failure "stop of P1-flow" with the power supply in intact condition, and $P_e(t)$ is the distribution function of the failure "loss of common power supply".

Two cause diagrams are coupled to the consequence diagram (as the cause of the common mode failure has been "extracted", there is no connection between these and the cause diagram of the "critical event"). One cause diagram gives as probability input the distribution function $P_{fu}(t)$ of the failure "P1 cannot start up" due to unrevealed fail-dangerous faults, and the other the distribution function of the failure "stop of P2-flow" due to an arisen fault.

Repair of P1 is in fig. 9 not taken into account, but it would be very easy to do it. In fig. 10 the diagram is shown for the case of repair of P1. It is assumed that change-over to a repaired P1 should not be carried out unless P2 stops (according to an existing procedure).

.....

A probability analysis of accidents in a nuclear power plant with large complex systems may in principle be carried out in a way similar to that in the simple example treated. The cause/consequence diagram method provides a basis from which analytical probability calculations can be made, but the method should perhaps first and foremost be regarded as a tool by means of which the problems are defined and presented. The use of simple, comprehensible symbols facilitates the communication between the "design engineer" and the "statistician" who perhaps later on, when the problems have been defined, prefers a "translation" to more abstract methods which may be more suitable for computer calculations.

ACKNOWLEDGEMENT

The author wants to thank his colleagues in the Electronics Department, especially Jens Rasmussen, Head of the Department, B. Runge, and P. Timmermann for inspiring discussions.

The interest of the Reactor Department is greatly appreciated, especially the discussions with H.E. Kongsø and P. Emmersen.

5. REFERENCES - LITERATURE

1. Farmer, F.R., Siting Criteria - a New Approach. Paper SM 89/34. . Containment and Siting of Nuclear Power Plants. Proceedings of a Symposium on the Containment and Siting of Nuclear Power Plants. Held by the International Atomic Energy Agency in Vienna, 3-7 April 1967 (IAEA, Vienna, 1967) 303-329.

2. Epler, E.P., *Common Mode Failure Considerations* in the Design of Systems for Protection and Control, Nuclear Safety, Volume 10, No. 1, 38-45, (Jan/Feb 1969).

3. Browning, R.L., Analyzing Industrial Risks, Chemical Engineering, 76, No. 23, 109-114 (Oct 20, 1969); No. 25, 239-244 (Nov 17, 1969); No. 27, 135-140 (Dec 15, 1969); 77, No. 2, 119-124 (Jan 26, 1970).

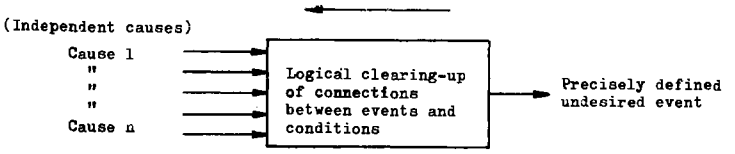
4. Schroder, R.J., Fault Trees for Reliability Analysis, BNWL-SA-2522 (Oct 1969).

5. Mieze, G., Reliability Analysis of Complex Systems with the Aid of the Fault-Tree Method, Kerntechnik, 12, Nr. 9, 377-387 (1970).

6. Knecht, O, und Keil, H., Graphische Analyse von Reaktorstörfällen, Atom und Strom, 14, 107-110 (Juli/August 1968).

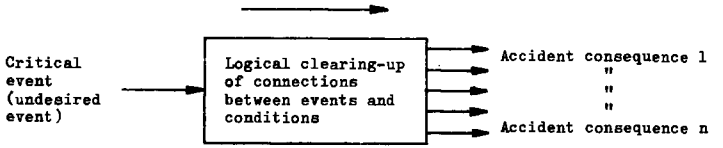
7. Green, A.E. and Bourne, A.J., Safety Assessment with Reference to Autcmatic Protective Systems for Nuclear Reactors, U.K.A.E.A. report AHSB(S)R117.

Construction direction of the diagram



The input and output data of the cause diagram

Construction direction of the diagram



The input and output data of the consequence diagram

Fig. 1

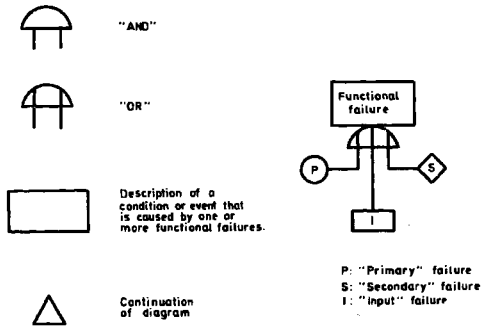
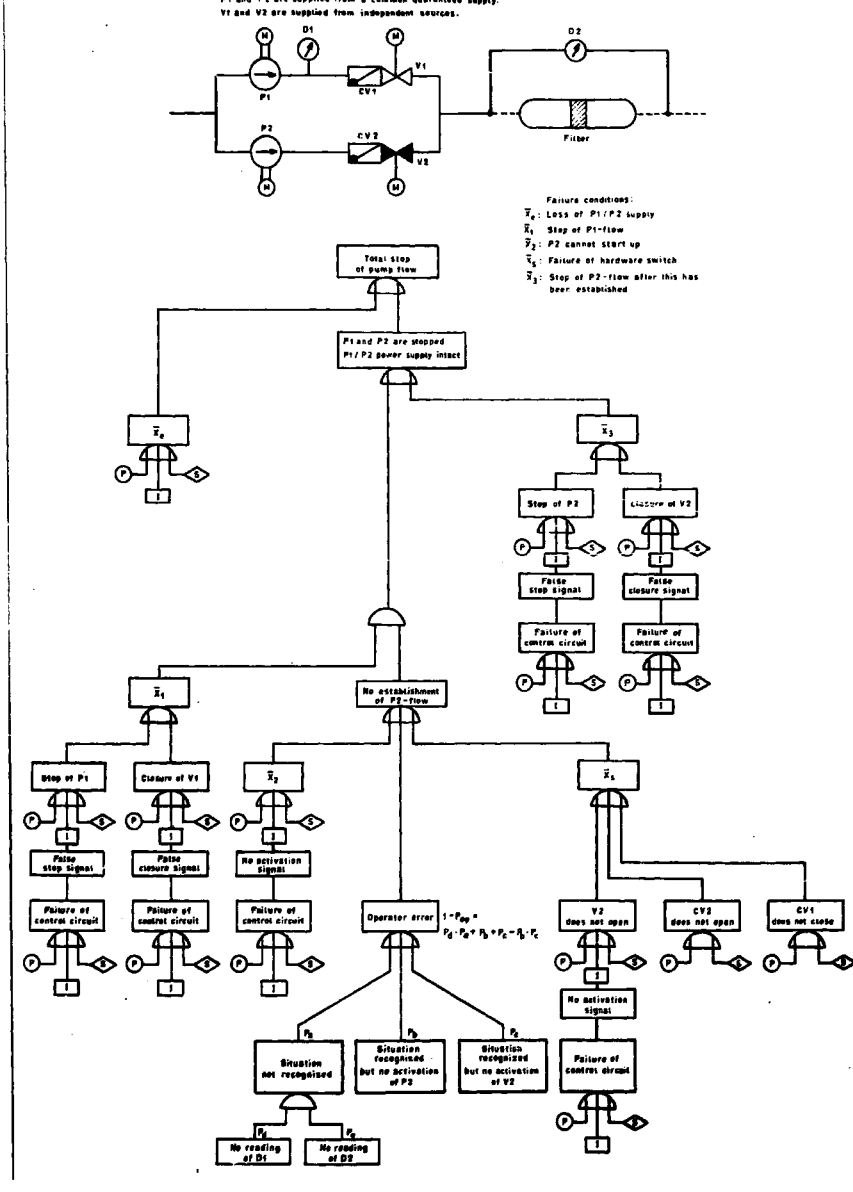


Fig. 2. Symbols used in the cause diagram.



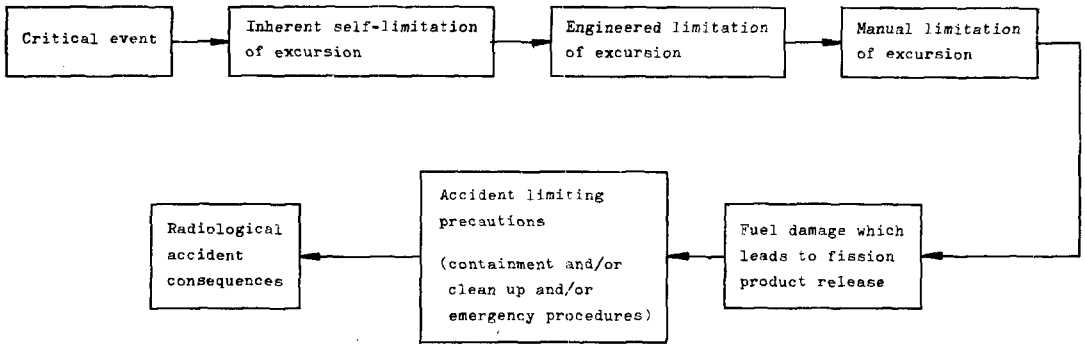


Fig. 4

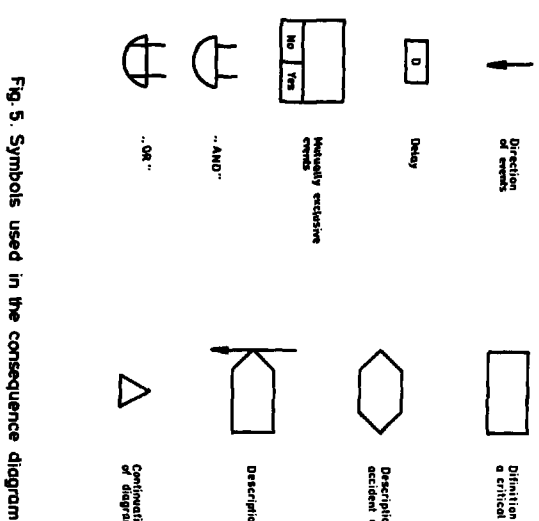
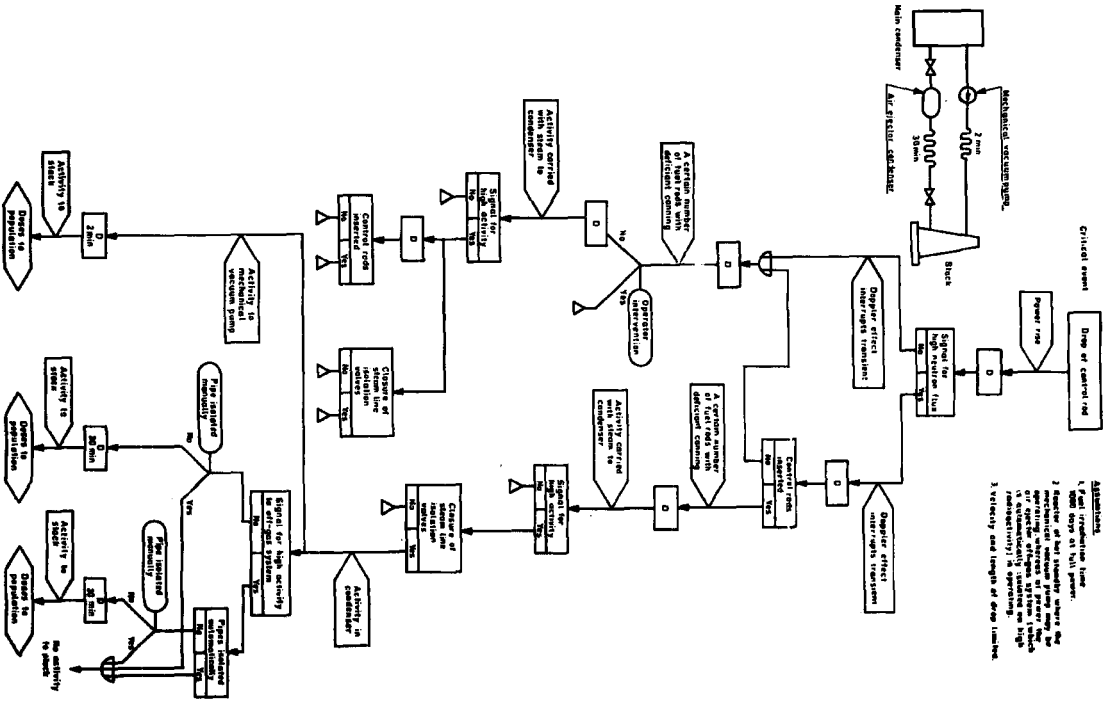


Fig. 5. Symbols used in the consequence diagram.



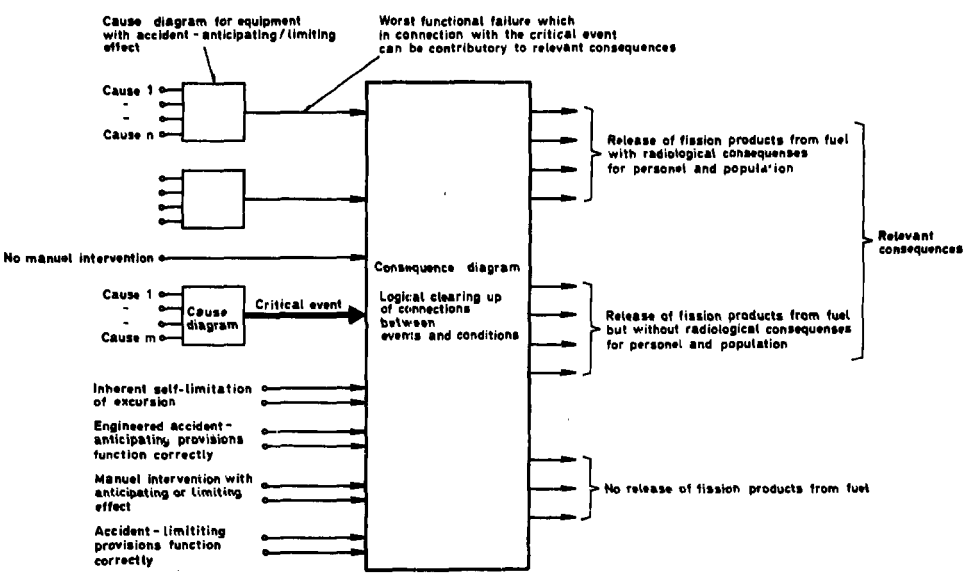


Fig. 7. Input / output data of the cause / consequence diagram

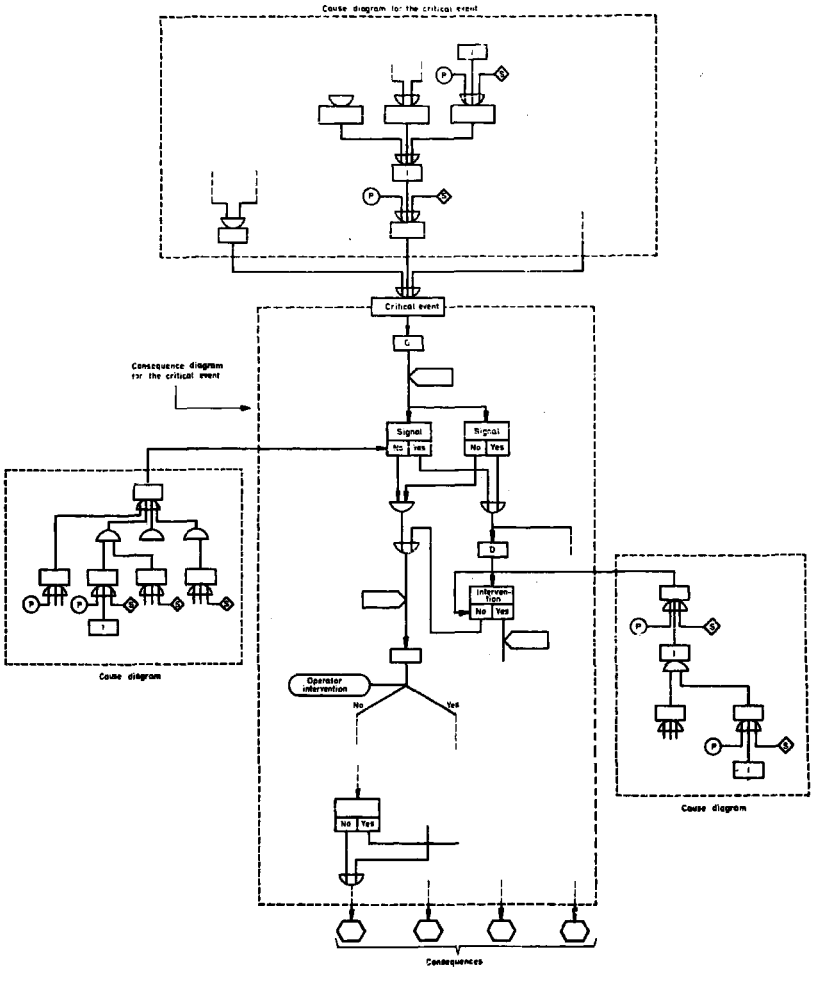


Fig. 8. The structure of a cause/consequence diagram.

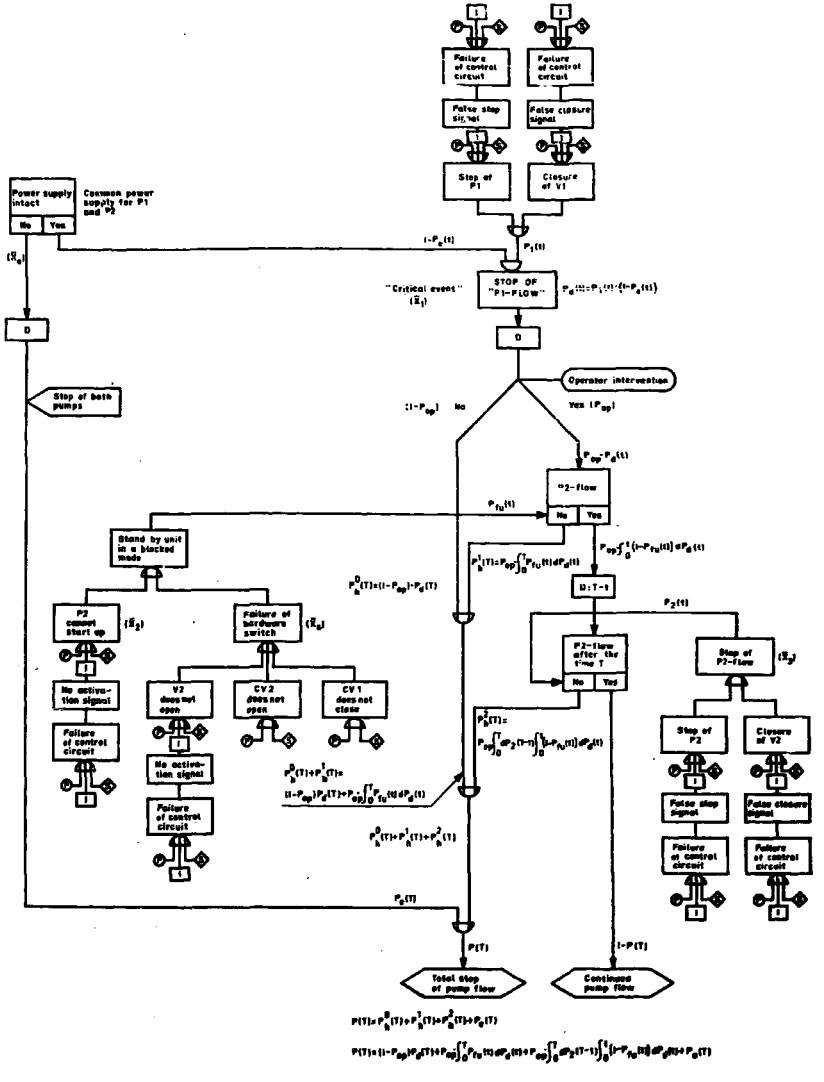


Fig. 9. Cause/consequence diagram for stand-by pump system.

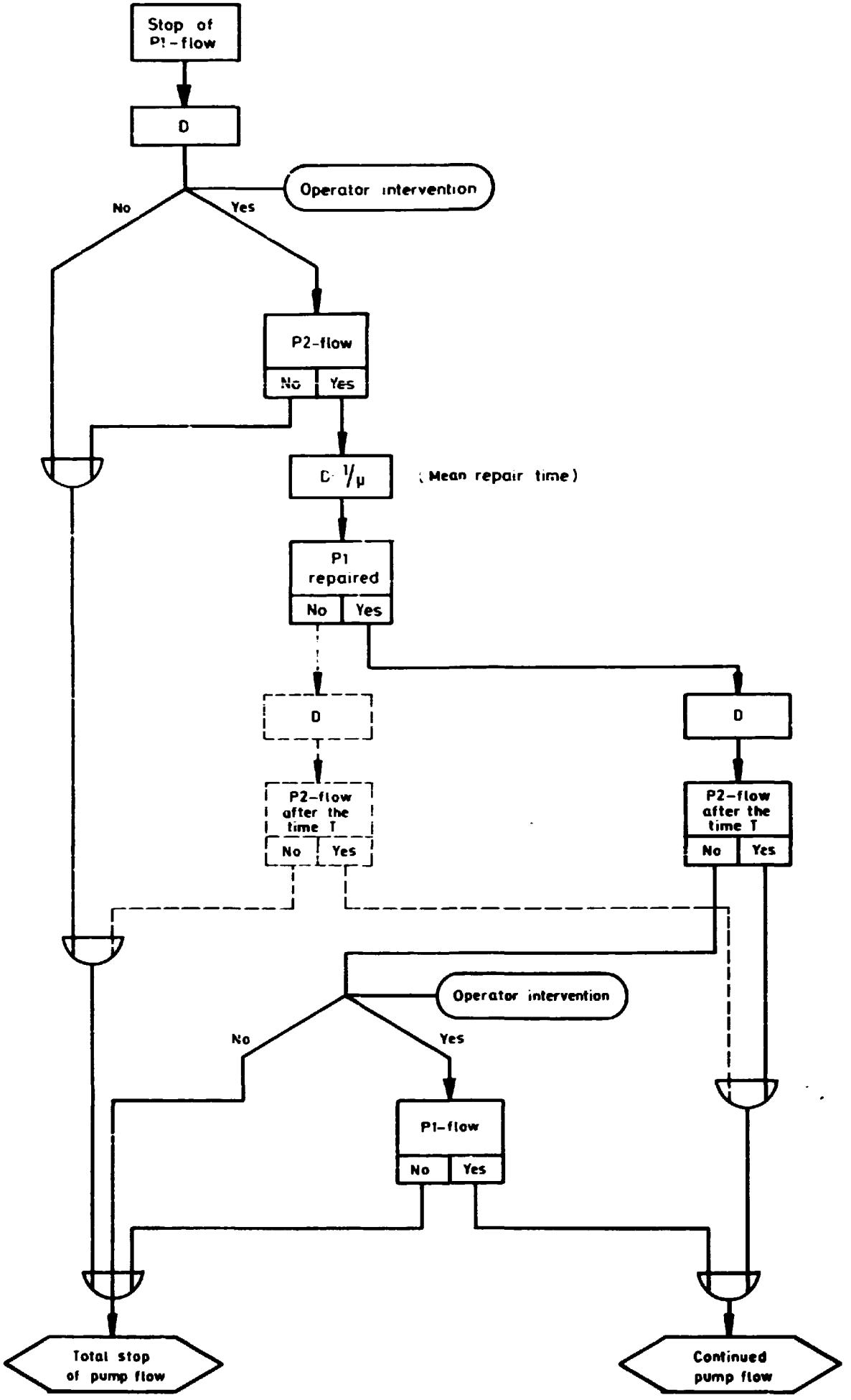


Fig. 10. Consequence diagram for stand-by pump system for the case of repair of P1.